CERTIFICATE OF TRANSMISSION BY FACSIMILE (37 CFR 1.8) Applicant(s): Gupta et al.	Docket No. JP920000150US1

Application No.	Filing Date	Examiner	Group Art Unit
09/626,637	7/27/2000	Shin, Kyung H.	2132

Invention: METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

I hereby certify that this Appeal Brief (23 pages)
(Identify type of correspondence)
is being facsimile transmitted to the United States Patent and Trademark Office (Fax. No. 703-872-9306

on 4/11/2005
(Date)

Kim Dwileski
(Typed or Printed Name of Person Signing Certificate)

(Signature)

Note: Each paper must have its own certificate of mailing.

TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. JP920000150US1

In Re Application Of: Gupta et al.

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/626,637	7/27/2000	Shin, Kyung H.	30449	2143	

Invention: METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

COMMISSIONER FOR PATENTS:

Transmitted herewith ~~in triplicate~~ is the Appeal Brief in this application, with respect to the Notice of Appeal filed on 2/11/2005

The fee for filing this Appeal Brief is: $500.00

☐ A check in the amount of the fee is enclosed.

☒ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 09-0457(IBM)

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Jack P. Friedman
Signature

Dated: 4/11/2005

Jack P. Friedman
Reg. No. 44,688
Schmeiser, Olsen & Watts
3 Lear Jet Lane, Suite 201
Latham, NY 12110
(518) 220-1850

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

cc:

P30LARGE/REV06

Docket No. JP920000150US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Gupta *et al.*

Group Art Unit: 2143

Filed: 7/27/2000

Examiner: Shin, Kyung H.

Serial No.: 09/626,637

Title: **METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANT

This Appeal Brief, pursuant to the Notice of Appeal filed September 9, 2004, is an appeal from the rejection of the Examiner dated August 11, 2004.

REAL PARTY IN INTEREST

International Business Machines, Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-6 and 11-19 are rejected. Claims 7-10 are canceled. This Brief is in support of an appeal from the rejection of claims 1-6 and 11-19.

STATUS OF AMENDMENTS

There are no After-Final Amendments which have not been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention discloses a method for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, but the authentication certificates of any of the server or browser are still valid. An original authentication certificate together with a server certifying authority chain (SCAC) certificate is received by the browser from the server during a SSL handshake between the browser and the server. The SCAC certificate was previously obtained by the server from the certifying authority. The browser verifies the original authentication certificate using the expired public key of the certifying authority. The browser verifies the SCAC certificate using a new public key of the certifying authority. See FIG. 1 (steps 1, 2, and 4) and specification, page 6, lines 9-10, 23-26; page 5, lines 5-10.

After verifying the original authentication certificate and after said verifying the SCAC certificate, the browser accepts the transaction between the browser and the server. See FIG. 1 (step 5) and specification, page 6, line 27 - page 7, line 2.

The SCAC certificate may be obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by: contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate; verifying the request by the certifying authority using the server's public key; and

generating the SCAC certificate by the certifying authority using a new private key of the certifying authority and forwarding the SCAC certificate to the server. See FIG. 2 and specification, page 7, lines 4-12.

Generating the SCAC certificate may include authenticating the server name, the server public key, old certifying authority public key, and certifying authority name. See specification, page 4, lines 24-26.

A client (CCAC) certificate may be issued by the certifying authority, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. The CCAC certificate may be presented to the server during the handshake. See specification, page 7, lines 16-22.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 4-6, 11, 13, and 17-19 stand rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Lewis et al. (U.S. Patent No. 6,233,565).

2. Claims 2-3 and 14-16 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis et al. (U.S. Patent No. 6,233,565) in view of Perlman et al. (U.S. Patent No. 6,230,266).

ARGUMENT

GROUND OF REJECTION 1

Claims 1, 4-6, 11, 13, and 17-19 stand rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Lewis et al. (U.S. Patent No. 6,233,565).

Claims 1, 5-6, 12-13, 17, and 19

Appellants respectfully contend that Lewis does not anticipate claims 1, 6, and 13, because Lewis does not teach each and every feature of claims 1, 6, and 13. For example, Lewis does not teach the following first feature: "receiving an original authentication certificate **together** with a server certifying authority chain (SCAC) certificate **by the browser from the server** during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority" (emphasis added) (claim 1), and similar language for claims 6 and 13.

The Examiner argues that Lewis discloses the aforementioned first feature of claims 1, 6, and 13. The Examiner relies specifically on content disclosed in Lewis, col. 30, lines 39-41. In response, Appellants respectfully contend that Lewis discloses in col. 30, lines 30-50 that the Certificate Authority (CA) first sends an "initial CA certificate" to the server, and after the old certificate has expired the Certificate Authority next sends a "new certificate" to the server. Thus it is clear that the "initial CA certificate" and the "new certificate" are not received **together** as required by claims 1, 6, and 13, but are instead received separately by the server. Specifically, Lewis recites in col. 30, lines 36-45:

> "**The initial CA's certificate** will be distributed by means of regular US certified mail. Included with the CA's certificate will be a hash of the next certificate key values. **When a certificate expires, the USPS certification authority will issue a new certificate** and sign it with the old certificates matching private key. The USPS CA will send a new certificate signed with the CA's new private key to the server 4. The server 4 will validate the certificate for authenticity by first checking to ensure that the new CA certificates public key authenticates the included signature." (emphasis added)

The preceding quote from Lewis discloses that "initial CA certificate" and the "new certificate" are received separately rather than together.

Also with respect to said first feature of claims 1, 6, and 13, the preceding quote from Lewis states that the old certificate and the new certificate are not received by the browser from the server as required by claims 1, 6, and 13, but are instead received by the server from the Certificate Authority.

Applicants assert that Lewis not disclose anywhere that the browser receives the old certificate and the new certificate together from the server during a SSL handshake.

In addition, Lewis does not teach the following second feature: "verifying by the browser the original authentication certificate using the **expired public key** of the certifying authority" (emphasis added) (claim 1), and similar language for claims 6 and 13. The Examiner argues that Lewis discloses the aforementioned second feature of claims 1, 6, and 13. The Examiner relies specifically on content disclosed in Lewis, col. 14, lines 36-42 and col. 30, lines 41-43. In response. Appellants respectfully contend that Lewis col. 14, lines 36-42 does not discuss verification of a certificate and is therefore totally irrelevant to aforementioned second feature of

claims 1, 6, and 13.

Furthermore, Appellants respectfully contend that Lewis col. 30, lines 41-43 states specifically that "[t]he USPS CA will send a new certificate signed with the CA's new private key to the server" which does not even mention an expired public key. The preceding second feature requires verification by the browser using the **expired public key** of the certifying authority, which Lewis does not teach. Although Lewis discloses in col. 27, lines 10-24 that a user may verify an X.509 certificate using a CA's public key, Lewis does not teach anywhere that the browser verifies the X.509 certificate using a public key **after the public key has expired** as required by claims 1, 6, and 13.

Based on the preceding arguments, Appellants respectfully maintain that Lewis does not anticipate claims 1, 6, and 13. Since claims 5 and 12 depend from claim 1, Appellants contend that claims 5 and 12 are likewise in condition for allowance. Since claims 17 and 19 depend from claim 13, Appellants contend that claims 17 and 19 are likewise in condition for allowance.

Claim 4

Since claim 4 depends from claim 1, which Appellants have argued *supra* to not be anticipated by Lewis, Applicants maintain that claim 4 is likewise not anticipated by Lewis.

In addition with respect to claim 4, Appellants maintain that Lewis does not teach the feature: "issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged". The Examiner argues that Lewis, col. 31, lines 30-38 teaches the

preceding feature of claim 4.

In response, Appellants maintain that Lewis, col. 31, lines 30-38 does not teach the preceding feature of claim 4, because Lewis, col. 31, lines 30-38 recites: "The cryptographic module 14 will retrieve the appropriate values from the SQL master database 305 and fill in the remaining values. The result is then signed with the client's private indicium key. The actual indicium 74 is the concatenation of data and the digital signature. Because of the presence of the client's certificate (which was signed by the USPS CA) the indicium 74 can be easily verified for authenticity by using the public key embedded in the client's 2 indicium certificate. "

Applicant's note that the indicia 74 appearing in the Examiner's citation of Lewis, col. 31, lines 30-38 is nothing more than a virtual postage stamp which does not relate to the preceding feature of claim 4. Lewis col. 12, lines 55-59 ("This virtual postage stamp is referred to as an "intelligent indicia 74" or more simply "indicia 74" and is evidence of payment for the postage that is locally printed and directly applied onto envelopes or labels via a printer ....").

Claims 11 and 18

Since claims 11 and 18 respectively depend from claims 1 and 13, which Appellants have argued *supra* to not be anticipated by Lewis, Applicants maintain that claims 11 and 18 are likewise not anticipated by Lewis.

In addition with respect to claims 11 and 18, Appellants maintain that Lewis does not teach the feature: "accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate" (claim 11), and similar language for claim 18. The Examiner argues that Lewis, col. 27, lines 10-24 teaches the

preceding feature of claims 11 and 18.

In response, Appellants maintain that Lewis, col. 27, lines 10-24 teaches that a user "A" may accept a transaction after verifying an authentication certificate, but does not teach that the user "A" would accept a transaction after verifying both the original authentication certificate and the SCAC certificate.

GROUND OF REJECTION 2

Claims 2-3 and 14-16 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis et al. (U.S. Patent No. 6,233,565) in view of Perlman et al. (U.S. Patent No. 6,230,266).

Claims 2 and 14

Since claims 2 and 14 respectively depend from claims 1 and 13, which Applicants have argued *supra* to not be anticipated by Lewis under 35 U.S.C. §102(c), Applicants maintain that claims 2 and 14 are not unpatentable over Lewis in view of Perlman under 35 U.S.C. §103(a).

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of Perlman does or suggest not teach the following first feature: "wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key". The Examiner argues that claim 1 of Perlman discloses the preceding first feature of claim 2.

In response, Appellants maintain that claim 1 of Perlman recites text relating to a first revocation server being compromised, but does not recite anything relating to the certifying authority invalidating its public key. In fact, the phrase "public key" does not even appear in claim 1 of Perlman. Therefore, the Examiner has not established a *prima facie* case of obviousness in relation to claims 2 and 14.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of Perlman does not teach or suggest the second feature: "contacting the certifying authority using

the server's private key for authentication **to make a request** for the SCAC certificate" (claim 2) (emphasis added), and similar language for claim 14. The Examiner argues that Perlman, col. 6, line 63 - col. 7, line 6 discloses the preceding second feature of claims 2 and 14.

In response, Appellants maintain that Perlman, col. 6, line 63 - col. 7, line 6 does not disclose "to make a request for the SCAC certificate", as alleged by the Examiner. Indeed, Perlman, col. 6, line 63 - col. 7, line 8 recites:

> "In order to update the certificates previously issued by certificate authorities 204c so as to ensure that principals relying upon such certificates now recognize the validity of certificates (including the special delegation certificate) issued by the successor CA 204b, CA 204a may issue, via secure off-line techniques, to certificate authorities 204c a **"renunciation" certificate** 600 (the data structure of which is represented in FIG. 6) signed using the private key of the CA 204a including information 602 stating that the CA 204a has renounced all of its certification authority (i.e., power to issue certificates), and has granted that authority to the CA 204b" (emphasis added).

Thus, Perlman, col. 6, line 63 - col. 7, line 6 discloses issuing a renunciation certificate and most certainly does not disclose requesting the SCAC certificate. In other words, "requesting" and "issuing" are different actions. Moreover, a renunciation certificate is not a SCAC certificate.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of Perlman does not teach or suggest the third feature: "verifying the request by the certifying authority using the server's public key" (claim 2), and similar language for claim 14. The Examiner argues that Perlman, col. 7, lines 15-18 discloses the preceding third feature of claims 2 and 14.

In response, Appellants maintain that Perlman, col. 7, lines 15-18 does not disclose "to make a request for the SCAC certificate", as alleged by the Examiner. Indeed, Perlman, col. 7, lines 15-18 recite: "The authorities 204c receiving such renunciation certificates from CA 204a verify that the renunciation certificates have been properly signed by the CA 204a". Appellants contend that the preceding quote of Perlman discloses verifying that the renunciation certificates have been properly signed by the CA, but does not disclose verifying the request by the certifying authority using the server's public key, as required by claims 2 and 14.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of Perlman does not teach or suggest the fourth feature: "generating the SCAC certificate by the certifying authority using a new private key of the certifying authority and **forwarding the SCAC certificate to the server**" (claim 2) (emphasis added), and similar language for claim 14. The Examiner argues that Perlman, col. 7, lines 12-24 discloses the preceding fourth feature of claims 2 and 14.

In response, Appellants maintain that Perlman, col. 7, lines 12-24 does not disclose "forwarding the SCAC certificate to the server" as alleged by the Examiner and as required by claims 2 and 14.

In addition, Appellants contend that the Examiner's reason for modifying Lewis by the alleged teaching of Perlman is not persuasive. The Examiner argues: "It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of *Lewis* to include a Certificate Authority (CA) that invalidates its key pair through the process of

revocation as taught in *Perlman*. One of ordinary skill in the art would have been motivated to incorporate the invention of Perlman in order to ensure the authenticity of certificates when a CA invalidates a public/private key pair due to a compromise in security. (see Perlman col. 2, lines 20-26: "*For complete network security, every principal must have a certificate. Sometimes, however, if is desirable to later disable a certificate after it has been issued but prior to its expiration. For example, a principal's private key may be stolen, compromised or lost, etc. Under such circumstances, it is desirable to revoke the certificate, thereby disabling authentication via that certificate.*")" (emphasis added)..

In response, Appellants maintain that the cited motivation in Perlman requires revocation of the original certificate ***prior to expiration*** of the original certificate. However, with respect to claims 1 and 13 from which claims 2 and 14 respectively depend, the Examiner cites Lewis, col. 30, lines 39-43 which requires that a condition precedent for issuance of the new certificate (alleged by the Examiner to be the SCAC certificate) is that the original certificate expires. See Lewis, col. 30, lines 39-43 ("**When a certificate expires,** the USPS certification authority will issue a new certificate ..." (emphasis added)).

Appellants contend that ordinary logic requires that the original certificate either have expired or not have expired (but not both) when the new certificate is issued by the CA. In other words, the Examiner is arguing to modify Lewis by the alleged teaching of Perlman by issuing the new certificate when the original certificate has both expired and not expired, which is logically impossible. Therefore, the Examiner's argument for modifying Lewis by the alleged teaching of Perlman is not persuasive.

Claims 3 and 15

Since claims 3 and 15 respectively depend from claims 1 and 13, which Applicants have argued *supra* to not be anticipated by Lewis under 35 U.S.C. §102(e), Applicants maintain that claims 3 and 15 are not unpatentable over Lewis in view of Perlman under 35 U.S.C. §103(a).

In addition with respect to claims 3 and 15, Appellants maintain that Lewis in view of Perlman does not teach or suggest the following feature: "wherein generating the SCAC certificate includes authenticating the server name, the server public key, old certifying authority public key, and certifying authority name" (emphasis added) (claim 3), and similar language for claim 15. The Examiner argues that Perlman, col. 7, lines 10-12 disclose the preceding feature of claims 3 and 15.

In response, Appellants maintain that Perlman, col. 7, lines 10-12 does not disclose authenticating all four items (the server name, the server public key, old certifying authority public key, and certifying authority name) listed in clams 3 and 15. In fact, Perlman, col. 7, lines 10-12 recites: "Additionally, in system 200, the new CA 204b is configured to issue certificates in the same name as the CA 204a", which is not a disclosure of authenticating all four items (the server name, the server public key, old certifying authority public key, and certifying authority name).

Claim 16

Since claim 16 depends from claim 13, which Applicants have argued *supra* to not be anticipated by Lewis under 35 U.S.C. §102(e), Applicants maintain that claim 16 is not

unpatentable over Lewis in view of Perlman under 35 U.S.C. §103(a).

In addition with respect to claim 16, Appellants maintain that Lewis in view of Perlman does not teach or suggest the following feature: "means for issuing by the certifying authority a client(CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged" (emphasis added). The Examiner argues that Lewis, col. 30, lines 59-62 disclose the preceding feature of claim 16.

In response, Appellants maintain that Lewis, col. 30, lines 59-62 does not disclose the preceding feature of claim 16, because Lewis, col. 30, lines 59-62 recites: "The USPS will generate the certificates and send them to the server 4, which will verify the certificate's source and store it in a SQL master database 305." Appellants contend that Lewis, col. 30, lines 59-62 does not relate to the preceding feature of claim 16.

SUMMARY

In summary, Appellant respectfully requests reversal of the August 11, 2004 Office Action rejection of claims 1-6 and 11-19.

Respectfully submitted,

Jack P. Friedman
Attorney For Appellant
Registration No. 44,688

Dated: 04/11/2005

Schmeiser, Olsen & Watts
3 Lear Jet Lane - Suite 201
Latham, New York 12110
(518) 220-1850

Docket No. JP920000150US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Gupta *et al.*
Filed: 7/27/2000
Serial No.: 09/626,637
Group Art Unit: 2143
Examiner: Shin, Kyung H.
Title: METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX A - CLAIMS ON APPEAL

1. A method for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority;

verifying by the browser the original authentication certificate using the expired public key of the certifying authority; and

verifying by the browser the SCAC certificate using a new public key of the certifying authority.

2. The method of claim 1, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate;

verifying the request by the certifying authority using the server's public key; and

generating the SCAC certificate by the certifying authority using a new private key of the certifying authority and forwarding the SCAC certificate to the server.

3. The method of claim 2 wherein generating the SCAC certificate includes authenticating the server name, the server public key, old certifying authority public key, and certifying authority name.

4. The method of claim 1, further comprising issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged.

5. The method of claim 1, wherein the method further comprises presenting the CCAC certificate to the server during the handshake.

6. In an arrangement of networked server and browser systems conducting secure transactions and including a certifying authority for authenticating such transactions, characterized in that it includes a means for authenticating transactions when the public and private key of the said certifying authority have expired but the authentication certificates of any of server or browser systems is still valid, comprising:

means for the server to obtain a certifying authority chain certificate using the new private key of the certifying authority,

means for presenting the said certifying authority chain certificate together with the original authentication certificate, to the browser,

means for verifying the original authentication certificate using the expired public key of the certifying authority, and verifying the certifying authority chain certificate using the new certifying authority public key by the browser.

11. The method of claim 1, further comprising accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate.

12. The method of claim 1, wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority.

13. A system for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

means for receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority;

means for verifying by the browser the original authentication certificate using the

expired public key of the certifying authority; and

means for verifying by the browser the SCAC certificate using a new public key of the certifying authority.

14. The system of claim 13, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

means for contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate;

means for verifying the request by the certifying authority using the server's public key; and

means for generating the SCAC certificate by the certifying authority using it's a new private key of the certifying authority and forwarding the SCAC certificate to the server.

15. The system of claim 13, wherein said means for generating the SCAC certificate includes means for authenticating the server name, the server public key, old certifying authority public key, and certifying authority name.

16. The system of claim 15, further comprising means for issuing by the certifying authority a client(CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged.

17. The system of claim 13, wherein the system further comprises means for presenting the

CCAC certificate to the server during the handshake.

18. The system of claim 13, further comprising means for accepting the transaction by the browser in conjunction with said means for verifying the original authentication certificate and in conjunction with said means for verifying the SCAC certificate.

19. The system of claim 13, wherein said means for obtaining the SCAC certificate comprises use of the new private key of the certifying authority.

Docket No. JP920000150US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Gupta *et al.*

Group Art Unit: 2143

Examiner: Shin, Kyung H.

Filed: 7/27/2000

Serial No.: 09/626,637

Title: METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX B - EVIDENCE

There is no evidence entered by the Examiner and relied upon by Appellants in this appeal.

Docket No. JP920000150US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Gupta *et al.*

Group Art Unit: 2143

Filed: 7/27/2000

Examiner: Shin, Kyung H.

Serial No.: 09/626,637

Title: **METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX C - RELATED PROCEEDINGS

There are no proceedings identified in the "Related Appeals and Interferences" section.